ABSTRACT

A security communication packet processing apparatus (100) comprises an encryption processing unit (102) that performs encryption processing and decryption processing in a data block unit of B1 bits, an authentication processing unit (104) that performs authentication processing in a data block unit of B2 (= n x B1) bits in parallel to the encryption processing or the decryption processing in the encryption processing unit (102) and outputs an authentication value, a data block accumulation unit (103) that accumulates the data blocks from the encryption processing unit (102) and outputs the data blocks to the authentication processing unit (104) when the accumulated amount of the data blocks reaches B2 bits, a packet construction unit (105) that reconstructs a packet with the data blocks from the encryption processing unit (102) and the authentication value from the authentication processing unit (104), and an encryption and authentication processing control unit (101) that divides the inputted packet into the data blocks of B1 bits and outputs the data blocks sequentially to the encryption processing unit.